REMARKS

In view of the following remarks, Applicant respectfully requests reconsideration and allowance of the subject application. This amendment is believed to be fully responsive to all issues raised in the May 06, 2004 Office Action.

Claim Amendments

Claims 11-16, 24-26, 29, 33, and 35 are cancelled. Claims 7-10, 17, 27, 30, and 32 are amended.

Rejections to the Claims

35 U.S.C. 112

Claim 15 is rejected under 35 U.S.C. 112, second paragraph, due to lack of sufficient antecedent basis for the recited limitation, "the control object".

Claim 15 has been canceled, rendering this rejection moot.

35 U.S.C. 102(e)

Claims 1, 2, 5, 7-10, 17, 18, and 20-23 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent Number 6,499,109 issued to Balasubramaniam et al. (herein referred to as "Bal").

Applicant's application describes techniques for limiting access to potentially dangerous code. A control object made up of executable code may be downloaded to a client device via a web page. Other web pages may then

attempt to execute the control object that was previously downloaded. To ensure that the control object is not invoked maliciously, Applicant's application describes authenticating the source of a web page that attempts to invoke the control object, and then verifying that the identified source is authorized to invoke the control object. The authentication is performed based on a digital signature that is associated with a web page that attempts to invoke the control object. The authorization may be performed in any of a number of ways, including, but not limited to, comparing the source of the web page with a list of authorized sources. If either the authentication or the authorization fails, then the control object is not invoked.

Specifically, claim 1 recites:

A method, comprising:

associating a digital signature with a web page; and

delivering the web page to an electronic device capable of authenticating the digital signature and executing at least a portion of the web page after the digital signature is authenticated

Bal describes verifying the source of software downloaded from a remote site to a client computer over a computer network before the software can be executed on the client computer. (Bal, Abstract.) Specifically, Bal describes a computer-executable program code that first determines the URL to which a browser running on the client computer is pointed and enables the downloaded software program only if the URL to which the browser is pointed is an

authorized URL. (Bal, Summary.) Bal is akin to a scenario Applicant describes in the Background section and upon which Applicant sought to improve with the claimed technique.

Bal does not describe "associating a ***digital signature with a web page***," nor does Bal describe "delivering the web page to an electronic device capable of ***authenticating the digital signature*** and executing at least a portion of the web page after the digital signature is authenticated," as claimed. The Office cites Bal, column 7, lines 32-38 as describing "associating a digital signature with a web page." Applicant respectfully disagrees, pointing out the column 7, lines 32-38 state, "initiating the downloading of a web page on the browser window on the client computer based on the URL, wherein the web page has associated therewith a control software program with a corresponding digital signature; verifying the control software program using the digital signature." This portion of Bal clearly states that a digital signature is associated with the control software program – ***not*** with the web page, as found in claim 1. Accordingly, claim 1 is allowable over Bal.

Claims 2-6 are allowable by virtue of their dependency on claim 1.

Claims 7-10 have been amended, rendering the rejection of claims 7-10 moot. Amended claim 7 clearly states that the web page has an associated digital signature, which, as stated above with reference to claim 1, is not described in Bal. Accordingly, claim 7, as amended, is allowable. Claims 8-10 are allowable by virtue of their dependency on claim 7.

Amended independent claim 17 recites:

17. A system, comprising:

a web browser configured to access a web page having a digital signature;

a processor configured to execute script contained in the web page;

an executable control object that may be invoked by the script in the web page and is executable on the processor; and

a confirmation module configured to authenticate the digital signature to determine based on authenticity of the digital signature, whether the control object should be invoked.

As stated above, Bal does not describe a ***web page*** having a digital signature. Rather, Bal describes a ***control object*** having a digital signature. Bal further describes examining a URL associated with a web page to determine whether or not the web page is authorized to invoke a particular control object. Bal does not describe authenticating a digital signature associated with a web page to determine whether or not the web page is authorized to invoke a control object. Nowhere does Bal describe "a web page having a digital signature " or "a confirmation module configured to authenticate the digital signature to determine based on authenticity of the digital signature, whether the control object should be invoked," as claimed. Accordingly, claim 17 is allowable over Bal.

Claims 18-23 are allowable by virtue of their dependency on claim 17.

Claims 11 and 14 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent Number 6,499,105 issued to Yoshiura et al. (herein referred to as "Yoshiura").

Claims 11 and 14 have been cancelled, rendering this rejection moot.

35 U.S.C. 103(a)

Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Bal in view of Yoshiura and further in view of U.S. Patent Number 6,058,482 issued to Liu (herein referred to as "Liu").

Claim 3 recites:

> The method as recited in claim 1, further comprising:
>
> determining if the web page includes code to invoke a control object; and
>
> deriving the digital signature and associating the digital signature with the web page only if the web page includes code to invoke a control object.

The Office contends that Bal discloses the method as recited in claim 1, that Yoshiura discloses determining if a mark with a digital signature should be derived and attached to a web page, and that Liu discloses determining if the web page includes code to invoke a control object. The Office further contends

that it would have been obvious to one having ordinary skill in the art to combine the teaching of Liu within the combination of Bal and Yoshiura. Applicant respectfully disagrees.

Specifically, none of the cited references disclose the method as recited in claim 1. Yoshiura describes a method for identifying a purchaser who purchased content from which an illegal copy was produced. (Yoshiura, Abstract.) Lui describes a server process for identifying a particular keyword in a web page, and then modifying the web page to enable secure download of executable code associated with the web page. The references fail to add any teaching to Bal regarding the recited features in claim 1. Namely, the combination of Bal, Yoshiura, and Liu fails to teach "associating a ***digital signature with a web page***" and "executing at least a portion of the web page after ***the digital signature*** is authenticated," as recited in claim 1.

Additionally, there is no suggestion to combine the teachings of Bal and Yoshiura. Yoshiura describes a method for identifying a purchaser who purchased content from which an illegal copy was produced. (Yoshiura, Abstract.) There is nothing in Yoshiura to suggest that identifying a purchaser of content has anything to do with authenticating access to executable code that may be invoked from a web page.

Furthermore, while Liu may disclose determining whether or not a web page includes code to invoke a control object, nowhere does Liu teach or suggest using that information to determine whether or not to generate and associate a digital signature with the web page. Rather, Liu discloses using

that information to determine whether or not to modify the web page to enable secure download of specific portions of executable code associated with the web page over a network. Liu describes processing that is performed in association with a web page that includes executable code that will need to be downloaded in order to be run. Liu does not suggest performing such processing in association with a web page that includes code that invokes a control object that may have already been downloaded. Accordingly, claim 3 is allowable over Bal in view of Yoshiura and further in view of Liu.

Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Bal in view of Yoshiura.

Claim 4 recites:

> The method as recited in claim 1, wherein the web page includes a confirmation module that is used by the electronic device to authenticate the digital signature.

The Office contends that Bal discloses the method as recited in claim 1, and that Bal in view of Yoshiura discloses wherein the web page includes a confirmation module that is used by the electronic device to authenticate the digital signature. Applicant respectfully disagrees.

Specifically, the combination of Bal and Yoshiura fails to teach the method as recited in claim 1. Specifically, the cited combination does not teach "associating a ***digital signature with a web page***," and "delivering the web

page to an electronic device capable of authenticating the ***digital signature*** and executing at least a portion of the web page after ***the digital signature*** is authenticated," as claimed. Furthermore, as noted previously, there is no motivation provided in the reference that would suggest combining the teachings of Bal and Yoshiura. Accordingly, claim 4 is allowable.

Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Bal in view of U.S. Patent Number 6,615,088 issued to Myer et al. (herein referred to as "Myer"). Myer describes a system that includes a master controller and one or more devices (e.g., a TV, a VCR, a CD changer, etc.) such that the master controller can be used to control the devices.

As described above, Bal does not teach or suggest the elements recited in claim 1, and Myer fails to add any teaching with respect to claim 1. Therefore, and by virtue of its dependence on claim 1, claim 6 is allowable over the combination of Bal and Myer.

Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Yoshiura in view of Liu.

Claim 12 has been cancelled, rendering this rejection moot.

Claims 13 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yoshiura in view of Bal.

Claims 13 and 16 have been cancelled, rendering this rejection moot.

Claim 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Yoshiura in view of Bal and further in view of U.S. Patent Number 5,958,051 issued to Renaud et al. (herein referred to as "Renaud").

Claim 15 has been cancelled, rendering this rejection moot.

Claims 19 and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bal in view of Renaud. The Applicant assumes that claims 26 and 32-35 were also intended to be included in this rejection, and are discussed herein as such.

Claims 24, 26, 33, and 35 have been cancelled, rendering the rejection of these claims moot.

Claim 19 recites:

> The system as recited in claim 17, wherein the confirmation module is included in the control object.

The Office contends that Bal discloses the system as recited in claim 17 and that Renaud discloses wherein the confirmation module is included in the control object. Applicant respectfully disagrees with this contention.

First, Bal does not disclose, teach, or suggest a ***web page*** having a digital signature, as recited in claim 17. Rather, Bal discloses a ***control object***

having a digital signature. Bal further discloses examining a URL associated with a web page to determine whether or not the web page is authorized to invoke a particular control object. Bal does not disclose, teach, or suggest authenticating a digital signature associated with a web page to determine whether or not the web page is authorized to invoke a control object. Nowhere does Bal disclose "a web page having a digital signature" or "a confirmation module configured to authenticate the digital signature" "wherein the confirmation module is called when the control object is invoked by the script, the control object executing only if the confirmation module authenticates the digital signature," as claimed. Accordingly, the elements recited in claim 17 are not disclosed in Bal.

Furthermore, Renaud discloses methods, apparatuses, and products that reduce the computational demands places on both source user computer systems and receiving user computer systems by requiring the implementation and the verification of only a single digital signature for an arbitrary number of data files. (Renaud, column 4, line 67 – column 5, line 4.) Renaud does not disclose, teach, or suggest a confirmation module included in a control object where the confirmation module is configured to authenticate a digital signature that is associated with a web page. Accordingly, the combination of Bal and Renaud does not teach or suggest the features of claim 17, from which claim 19 depends.

The Office cites Renaud column 4, lines 15-19 as disclosing "wherein the confirmation module is included in the control object," as recited in claim 19. The cited portion of Renaud states:

> "In another embodiment, computer-readable program code includes code for running the applet and code for determining whether the applet performs an action that triggers a security check. In another embodiment, code is included for use in establishing a secure connection with a remote site."

The cited text in no way teaches or suggests a confirmation module included in a control object, as claimed. Accordingly, and by virtue of its dependence on claim 17, claim 19 is therefore allowable.

Amended claim 32 recites:

> A control object stored in a computer-readable medium, comprising computer-executable instructions that, when executed on a computer, perform the following:
>
> authenticating a web page that invokes the control object, wherein the authenticating is performed based on a digital signature associated with the web page; and
>
> executing a data-handling task on the computer if the web page is determined to be authentic.

As amended, claim 32 clearly recites that "the authenticating is performed based on a digital signature associated with the web page". As discussed above with reference to claim 3, neither Bal nor Renaud disclose, teach, or suggest a web page having an associated digital signature, nor authenticating a web page based on a digital signature that is associated with the web page. Accordingly, claim 32, as amended, is allowable.

Claim 34 is allowable by virtue of its dependence on claim 32.

Claim 25 is rejected under 35 U.S.C. 103(a) as being unpatentable over Bal in view of Renaud and further in view of Yoshiura.

Claim 25 has been cancelled, rendering this rejection of claim 25 moot.

Claims 27-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bal in view of Liu.

Claims 27 and 30 have been amended and claim 29 has been cancelled. Accordingly, the rejection of claims 27-31 are moot.

Conclusion

Claims 1-10, 17-23, 27, 28, 30-32, and 34 are believed to be in condition for allowance. Applicant respectfully requests reconsideration and prompt issuance of the present application. Should any issue remain that prevents

immediate issuance of the application, the Examiner is encouraged to contact the undersigned agent to discuss the unresolved issue.

Respectfully Submitted,
Lee & Hayes, PLLC
421 W. Riverside Avenue, Suite 500
Spokane, WA 99201

Dated: 7/29/04

Kayla D. Brant

Name: Kayla D. Brant
Reg. No. 46,576
Phone No. (509) 324-9256 ext. 242